High Performance Event Detection Server

User Manual

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (http://www.hikvision.com).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks Acknowledgement

- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

Laws and Regulations	Use of the product must be in strict compliance with the local laws and regulations. Please shut down the device in prohibited area.
Power Supply	• Use of the product must be in strict compliance with the local electrical safety regulations. • Use the power adapter provided by qualified manufacturer. Refer to the product specification for detailed power requirements. • It is recommended to provide independent power adapter for each device as adapter overload may cause over-heating or a fire hazard. • Make sure that the power has been disconnected before you wire, install, or disassemble the device. • DO NOT directly touch exposed contacts and components once the device is powered up to avoid electric shock. • DO NOT use damaged power supply devices (e.g., cable, power adapter, etc.) to avoid electric shock, fire hazard, and explosion. • DO NOT directly cut the power supply to shut down the device. Please shut down the device normally and then unplug the power cord to avoid data loss. • DO NOT block the power supply equipment to plug and unplug conveniently. • Make sure the power supply has been disconnected if the power adapter is idle. • Make sure the device is connected to the ground firmly.

Transportation, Use, and Storage	● To avoid heat accumulation, good ventilation is required for a proper operating environment. ● Store the device in dry, well-ventilated, corrosive-gas-free, no direct sunlight, and no heating source environment. ● Avoid fire, water, and explosive environment when using the device. ● Avoid lightning strike for device installation. Install a lightning arrester if necessary. ● Keep the device away from magnetic interference. ● Avoid device installation on vibratory surface or places, and avoid equipment installation on vibratory surface or places subject to shock (ignorance may cause device damage). ● DO NOT touch the heat dissipation component to avoid burns. ● DO NOT expose the device to extremely hot, cold, or humidity environments. For temperature and humidity requirements, see device specification.
Maintenance	● If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center. ● If the device is abnormal, contact the store you purchased it or the nearest service center. DO NOT disassemble or modify the device in any way (For the problems caused by unauthorized modification or maintenance, the company shall not take any responsibility). ● Keep all wrappers after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage to the device and the company shall not take any responsibility.
Network	● Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Please contact us when the device might exist network security risks. ● Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.
Data	DO NOT disconnect the power during formatting, uploading, and downloading. Or files may be damaged.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Product Introduction

Event detection server, the multiple-channel video analysis device, provides multiply features, including events smart detection and traffic parameters collection. It can capture for detected events, and recognize license plate. It is widely applied in real-time detection in cities, highways, and tunnels, etc.

1.2 Key Feature

- Box camera and speed dome are connectable.
- Rack-mounted 1U chassis design, makes server convenient to place in cabinet of server room.
- Supports multiple events detection.
- Supports traffic parameters collection.
- Supports illegal parking zoom capture and multiple scenes patrol detection when speed dome is connected.
- Supports operation via Web.
- Supports customizing specific events detection.

1.3 System Requirement

- Web Browser: IE 9.0 and above versions.
- Resolution: 1024 × 768 and above.

Chapter 2 Getting Started

2.1 Start Up and Shut Down

Purpose:

Proper startup and shutdown procedures are crucial to expanding the life of the device.

2.1.1 Start Up

Before you start:

- Fix the device in an equipment cabinet.
- Ensure the device is properly grounded.
- Plug the network cable.

Plug the power supply to start up.

NOTE

Make sure the power supply is plugged into an electrical outlet. It is highly recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device.

2.1.2 Shut Down

Unplug the power supply to shut down.

2.2 Set Admin Password

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP or Client Software.

Before you start:

Set the IP address of your computer. Make sure the device is in the same network segment with your computer.

Step 1 Enter device IP address in address bar of the browser and press **Enter**. Thus the activation interface pops up.

Step 2 Enter the **Admin Password** and **Confirm Password**.

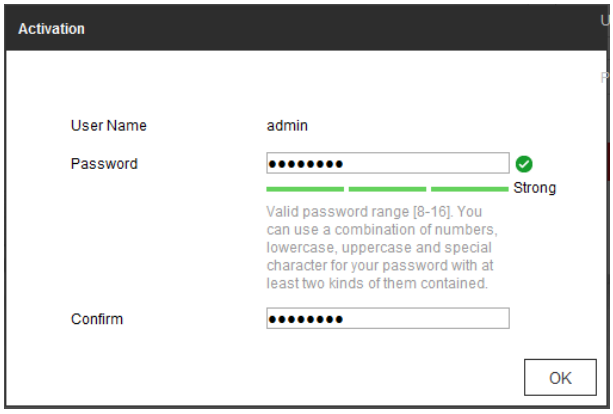

Figure 2-1 Set Admin Password

WARNING

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 3 Click OK to set the admin password.

Step 4 After successful login, follow the prompt to install the plug-in.

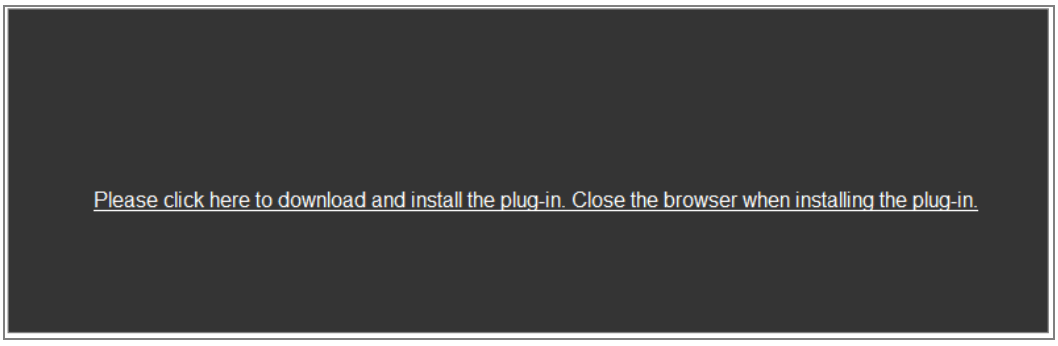

Figure 2-2 Installing Plug-in

Chapter 3 Configure Network

Purpose:

Guarantee the network connection between your computer and the device is correct, thus you can control the device remotely.

3.1 Configure Port

NOTE

The terminal device which is listened, should be set as listened mode.

Step 1 Go to **System > Sys Config > Basic Configuration**.

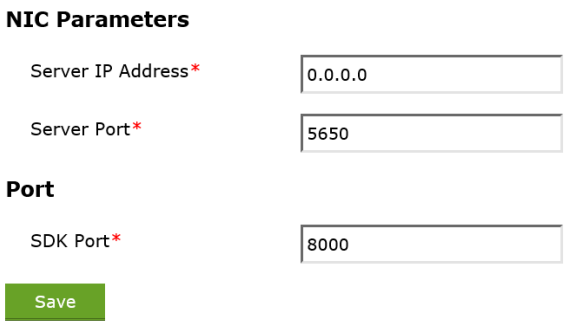

Figure 3-1 Port Configuration

Step 2 Edit the Server IP Address, Server Port, and SDK Port.

Step 3 Click **Save** to save the settings.

NOTE

Reboot the device to activate the new settings.

3.2 Configure Network

Step 1 Go to **Network**, you can view smart analysis unit information and status.

Step 2 Check **UID Indicator**, to rapidly locate the server.

Step 3 Go to **Network > Local > Configuration > Basic Configuration**, to edit the basic network settings.

Step 4 Go to **Network > Local > Configuration > Network Configuration > LAN**.

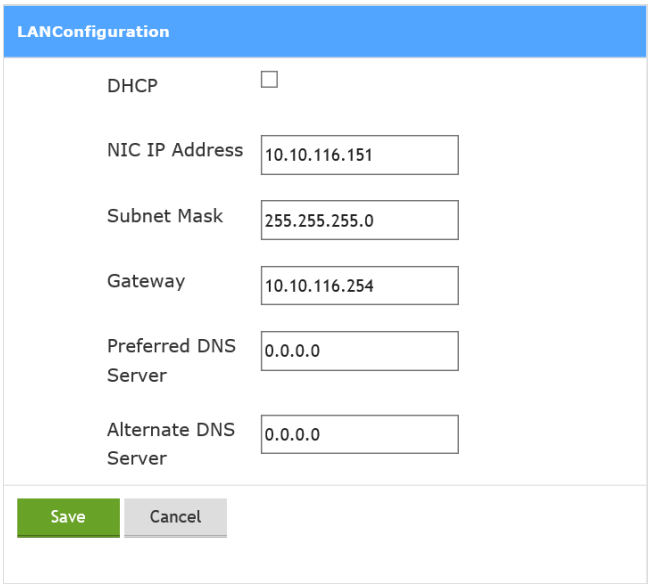

Figure 3-2 LAN Configuration

1) Enable **DHCP**.
2) Set NIC IP address, subnet mask, gateway, preferred DNS server, and alternate DNS server.
3) Click **Save** to save the settings.

Step 5 Go to **Network > Local > Performance**, to view **CPU Usage Rate**, **Network IO** and **Temperature**.

Step 6 (Optional)Click **Reboot** or **Disable**, to reboot or disable the server.

NOTE

Only desktop computer is supported to directly connect port.

Chapter 4 Event Detection Configuration

4.1 Live View Operations

Go to live View, select the channel for live view.

4.2 Configure Camera

4.2.1 Confiugre Camera Parameter

Purpose:

Configure camera parameter to collect and capture pictures.

Step 1 Go to **Channel Config > Camera Parameter**.

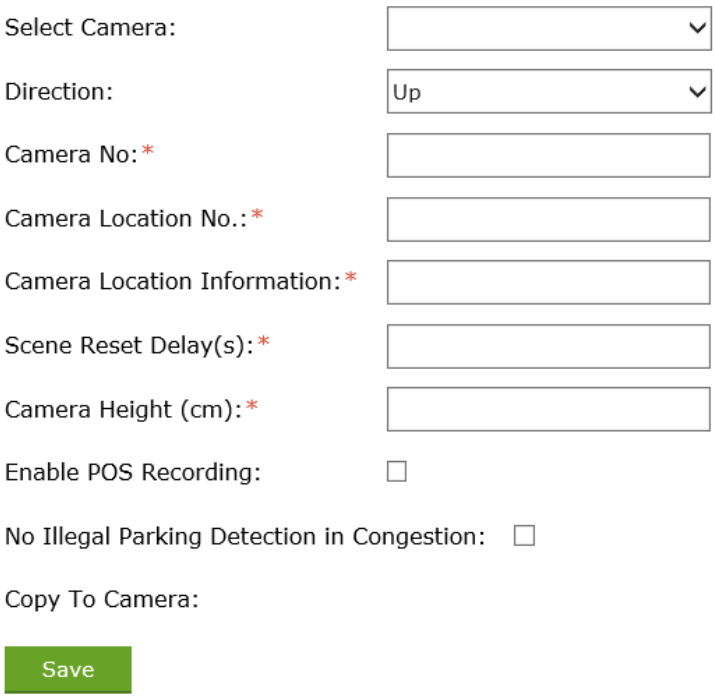

Figure 4-1 Camera Parameter Configuration

Step 2 Select the camera.

Step 3 Configure camera parameters according to actual demand.

Step 4 Click **Save** to save the settings.

4.2.2 Confiugre Picture Composition

Purpose:

Configure picture composition to set image collage layout.

Step 1 Go to **Channel Config > Picture Composition**.

Step 2 Select camera to configure.

Step 3 Set Compose as **Enable**.

Step 4 Select layout for **2 Captured Pictures**, **3 Captured Pictures** and **4 Captured Pictures**.

Step 5 Click **Save** to save the settings.

4.2.3 Configure Information and Text Overlay

Purpose:

Overlay text on composite pictures.

Step 1 Go to **Channel Config > Information and Text Overlay**.

Step 2 Select camera to configure.

Step 3 Select **Overlay Method**.

Step 4 Set text parameters including **Stacking Line Percentage, Initial Top Margin, Initial Left Margin, Spaces After Overlay Items, Character Size, Character Spacing, Foreground RGB Value, Background RGB Value**.

- **Initial Top Margin**: Text position from top margin.
- **Initial Left Margin**: Text position from left margin.
- **Stacking Line Percentage**: Text will switch to next line when the percentage between text length and picture width reaches the set value.

Step 5 Select Overlay Content.

Step 6 Click **Save** to save the settings.

4.2.4 Configure Scene

Purpose:

Configure Scene to collect traffic data, illegal parking evidence, detect event in road.

Step 1 Go to **Channel Config > Scene Configuration > Scene**.

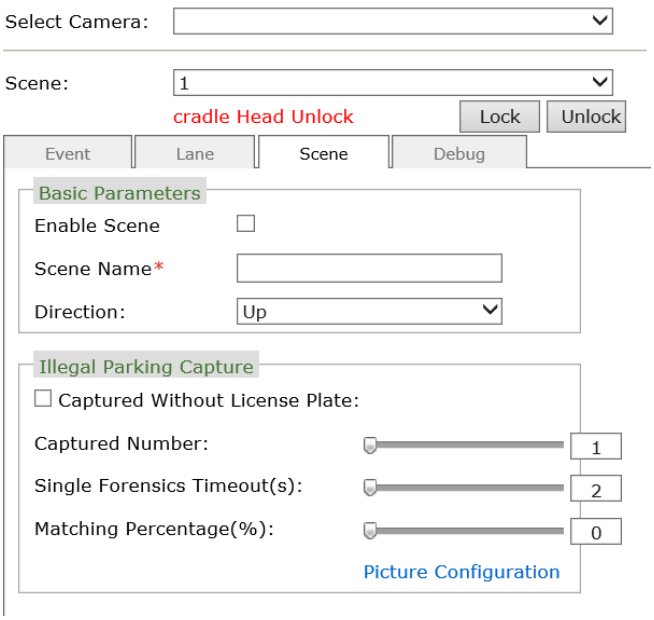

Figure 4-2 Scene Configuration

Step 2 Select camera according to actual demand.

Step 3 Select scene according to actual demand.

Step 4 Set focus by adjust the PTZ panel buttons.

NOTE

Illegal parking evidence is supported when accessing speed dome.

Step 5 Select scene name and direction according to actual demand.

Step 6 Click **Save** to save the settings.

Step 7 (Optional) Copy the settings to other cameras.

NOTE

Go to **Channel Config > Scene Cruise**, to set scene details.

Configure Illegal Parking Evidence

Purpose:

Configure illegal parking evidence to detect vehicle in illegal detection areas and collect illegal parking evidence

NOTE

Illegal parking evidence is supported when accessing speed dome.

Step 1 Go to **Channel Config > Scene Configuration > Scene > Illegal Parking Capture**.

Step 2 (Optional) check **Captured Without License Plate**.

Step 3 Set **Captured Number**, **Single Forensics Timeout** and **Matching Percentage**.

Step 4 Click **Picture Configuration**, set **Capture Interval** and **Capture Type**.

Step 5 Click **Save** to save the settings.

Configure Traffic Event Rules

Purpose:

Configure traffic event rules to detect vehicle and collect violation evidence.

Step 1 Go to **Channel Config > Scene Configuration > Event**.

Step 2 Select **Camera**, **Scene** and **Scene Mode**.

Step 3 Draw area.

1) Click **Draw Area**.
2) Click and drag the mouse on the view screen to draw a red rectangle, and right click to finish drawing.

Step 4 Enable event according to actual need. Checked events will be analyzed and detected.

NOTE

Event **Flow** must be checked when detecting congestion, queue jumping and event detection. When enable flow detection, drawed flow triggered line and lane line should be crossed.

Step 5 Set event detection parameters according to actual need.

Step 6 Click **Save** to save the settings.

Configure Lane

Purpose:

Set lane before enabling traffic data collection.

NOTE

Two lane lines should be set in each lane, and up to 6 lanes can be set in a scene. No neighboring lanes crossing are allowed.

Step 1 Go to **Channel Config > Scene Configuration > Lane**.

Step 2 Select channel.

Step 3 Select lane number.

Step 4 Click left line and right line to draw lane lines in videos according to actual lanes.

Step 5 Click **Configure Lane Information**, and select lane type and lane direction.

Step 6 Click **Save** to save the settings.

Configure Manual Evidence Capture

Purpose:

Configure manual evidence capture to detect evidence data.

Step 1 Go to **Channel Config > Manual Evidence Capture**.

Step 2 Select channel.

Step 3 (Optional) Check **Captured Without License Plate** according actual need.

Step 4 Set **Capture Number**, **Single Forensics Timeout** and **Matching Percentage**.

Step 5 Click **Picture Configuration**, to set capture interval and picture type.

Step 6 Click **Save** to save the settings.

Step 7 (Optional) Go to **Live View**, click "  " to capture manually.

Configure Scene Patrol

Purpose:

Configure scene patrol, the terminal device will monitor in specified scenes.

Step 1 Go to **Channel Config > Scene Cruise**.

Step 2 Select camera.

Step 3 Enable **Cruise Plan**.

Step 4 Set cruise plan start time and end time.

NOTE

Up to 16 cruise period are supported.

Step 5 Click **Details** to set more settings.

Step 6 Click **Save** to save the settings.

Step 7 (Optional) Copy the settings to other cameras.

NOTE

Scene cruise is supported when accessing speed dome.

4.3 Configure FTP

Purpose:

Configure the FTP parameters, to upload data to FTP servers.

Before you start:

FTP server is constructed and well connected with network.

Step 1 Go to **System > System Config > FTP Upload**.

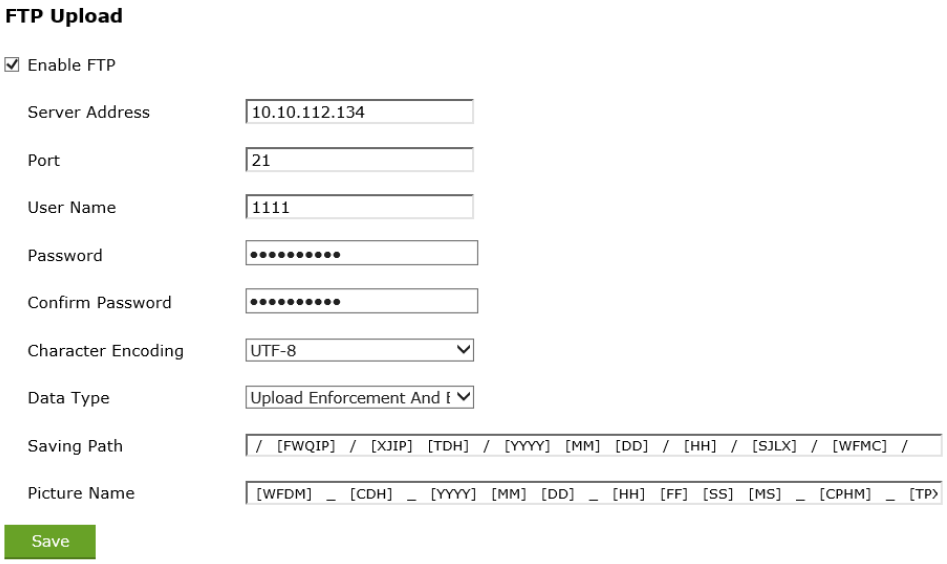

Figure 4-3 FTP Configuration

Step 2 Enable **FTP**.

Step 3 Set **Port**, **User Name**, and **Password**.

Step 4 Set data uploading.

1) Set **Data Type**.
2) Set **Saving Path** and **Picture Name**.

Step 5 Click **Save** to save the settings.

Chapter 5 Maintenance and Management

5.1 User Management

Purpose:

You can add, edit, and delete users.

5.1.1 Add a User

Step 1 Go to **System > Sys Config > User Configuration**.

Step 2 Click **Add** to enter the Add user interface.

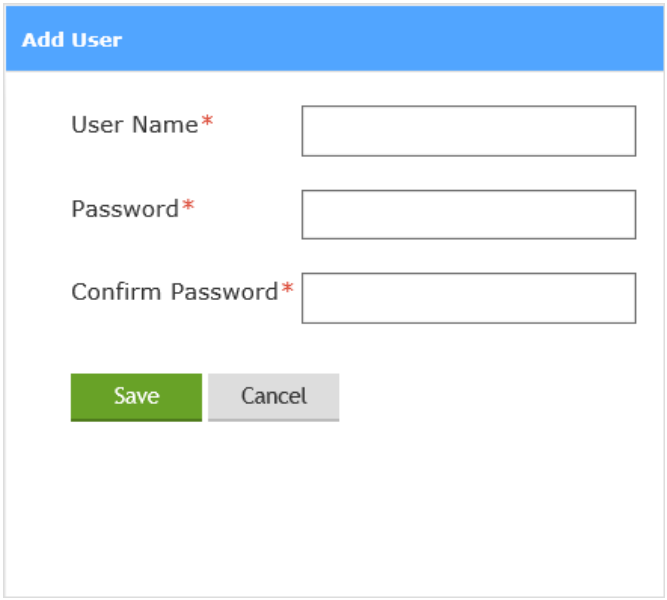

Figure 5-1 Add User

Step 3 Enter the **User Name** and **Password**, and confirm the password.

WARNING

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 Click **Save** to save the settings.

5.1.2 Edit a User

NOTE

You need the admin password to edit the admin user.

Step 1 Select a user account.

Step 2 Click the user name to enter the setting interface.

Step 3 Modify the **User Name**, and **Password**.

WARNING

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 Click **Save** to save the settings.

5.1.3 Delete a User

Step 1 Select a user account from the list on the User Information interface to be deleted.

Step 2 Click **Delete**.

Step 3 Click **OK** to delete the selected user account.

5.2 Device Management

Purpose:

You can restart, restore default, repair database index, export/import configuration file, and upgrade device.

5.2.1 View Device Status

Go to **Resourses**, to view the device status, including device name, type, IP address, port, and online status.

5.2.2 Add or Delete Device

Go to **Resourses**, select the device, and click **Add** or **Delete**.

5.2.3 Import or Export Device

Go to **Resourses**, select the device, and click **Import** or **Export**.

5.2.4 View Version

Go to **System > Version**, and you can view device versions and plug-in information.

5.3 Time Synchronization

When the server time is inaccurate, you can configure the time synchronization according to connected platform.

Step 1 Go to **System > Sys Config > Time Configuration**.

Step 2 Select time synchronization type, and set time synchronization parameters.

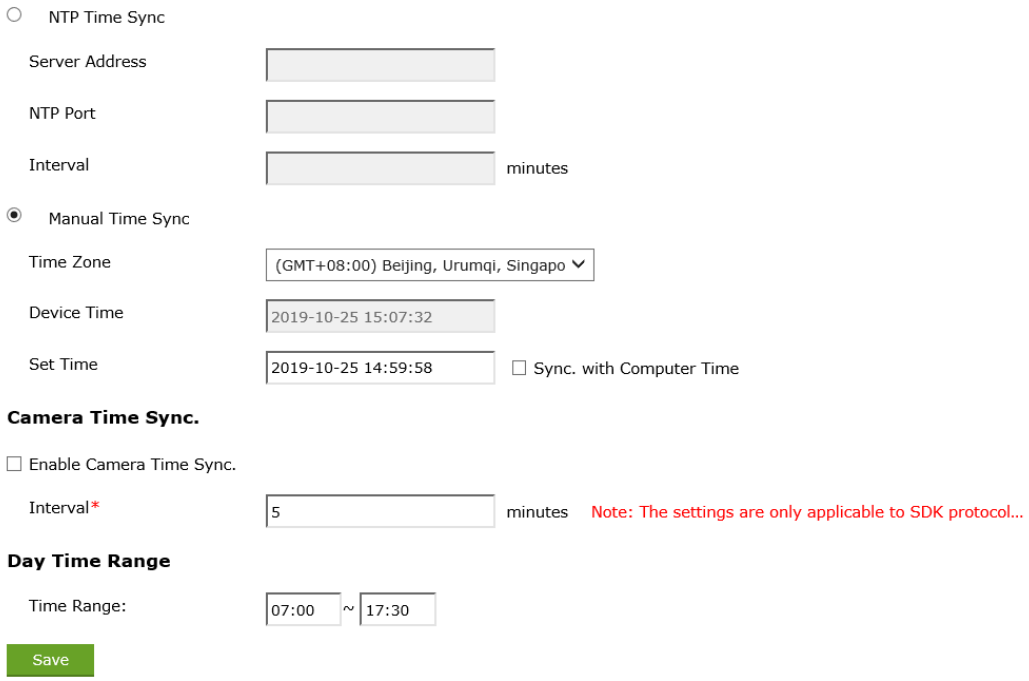

Figure 5-2 Time Synchronization

NOTE

The server can only adopt one time synchronization type. Camera time synchronization is only applicable to SDK protocol.

5.4 Log Management

Purpose:

The operation and alarm information of the server can be stored in log files. You can also export the log files according to actual need.

Before you start:

Please insert a memory card with in the camera for Log storage. Log cannot be searched if there is no memory card.

Step 1 Go to **System > Log**.

Step 2 Select log type.

Step 3 Set the **Start Time**, and **End Time**.

Step 4 Click **Search**.

Step 5 (Optional) Export the log files.

1) Click **Export**.
2) Set **Saving Path** and **Log Name**.
3) Click **Save** to save the settings.

5.5 Upgrade

Purpose:

Configure upgrade to upgrade the system.

Please do not disconnect power to the device during the process. The device reboots automatically after upgrading.

Step 1 Go to **System > Upgrade**.

Step 2 Select the smart analysis unit, and click **Next**.

Step 3 Select the upgrade file, and click **Next**.

Step 4 Click **Upgrade**.

5.6 Restore Default Settings

Purpose:

Restore default settings when parameters are incorrect.

Step 1 Go to **System > Sys Config > Default Configuration**.

Step 2 Select restore type.

- **Simply Restore**: Restore basic parameters, except IP address, subnet mask, gateway and port.
- **Restore All**: Restore all parameters.

Step 3 Click **Save** to save the settings.

0300101091026


See Far, Go Further